

# METHOD FOR TRACING TRAITOR RECEIVERS IN A BROADCAST ENCRYPTION SYSTEM

## ABSTRACT OF THE DISCLOSURE

A method for tracing traitor receivers in a broadcast encryption system. The method includes using a false key to encode plural subsets representing receivers in the system. The subsets are derived from a tree using a Subset-Cover system, and the traitor receiver is associated with one or more compromised keys that have been obtained by a potentially cloned pirate receiver. Using a clone of the pirate receiver, the identity of the traitor receiver is determined, or the pirate receiver clones are rendered useless for decrypting data using the compromised key by generating an appropriate set of subsets.